The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
07/10/2012

SUBJECT:
Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (MS12-045)

OVERVIEW:
A vulnerability has been discovered in the Microsoft Data Access Components (DAC) that could allow remote code execution which may permit an attacker to take complete control of an affected system. Microsoft Data Access Components is a collection of components that allow for programs to access databases and to manipulate the data. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Microsoft Data Access Components 2.8
- Microsoft Data Access Components 6.0
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003 (except Server Core installations)
- Microsoft Windows Server 2008 (except Server Core installations)

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the Microsoft Data Access Components (DAC) an attacker to take complete control of an affected system. This vulnerability exists because DAC attempts to access an object in memory that has not been initialized resulting in potential memory corruption. To exploit this vulnerability, an attacker creates a specially crafted website, and have users visit that web site or click on a link in an email. In addition, compromised websites as well as websites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

By default, Internet Explorer on Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 runs in a restricted mode, which mitigates this vulnerability. Restricted mode is also known as Enhanced Security Configuration.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems after testing.
- Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/MS12-045

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1891

Security Focus:

http://www.securityfocus.com/bid/54308